IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Crim. No. 19-262
	)	
PAUL CHRETIEN,	)	
Defendant.	)	

FINDINGS OF FACT AND CONCLUSION OF LAW

CONTI, Senior District Judge

I. INTRODUCTION

Pending before the court is a motion to suppress evidence (ECF No. 29) filed by defendant Paul Chretien ("Chretien"). Chretien is charged in a criminal indictment with: (1) distribution of material depicting the sexual exploitation of a minor on various dates in September and November, 2018, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) (counts 1-3 and 5-6); (2) receipt of material depicting the sexual exploitation of a minor on or about August 22, 2018, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) (count 4); and (3) possession of material depicting the sexual exploitation of a minor on or about February 6, 2019, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (count 7). The charges in the indictment are based upon evidence that was obtained pursuant to a search warrant issued by a state court judge and conducted at Chretien's home. The application for the search warrant was issued based upon an affidavit of probable cause authored by Steven Dish ("Dish"), a detective for the Allegheny County Police Department.

According to Chretien, the search warrant was not supported by probable cause because, among other reasons, the information contained in Dish's affidavit of probable cause is stale. Chretien argues that under those circumstances his rights guaranteed by the Fourth Amendment to the United States Constitution were violated and the evidence obtained from the search warrant,

including any incriminating statements made to law enforcement after the execution of the search warrant, should be suppressed. The government opposes Chretien's motion and argues that based upon the nature of Chretien's alleged child pornography crimes, including the technology used to commit those crimes and the clandestine nature of the crimes, the information contained in the affidavit of probable cause was not stale and there existed a substantial basis for the state court judge's determination that probable cause existed to search Chretien's home for evidence of a violation of 18 PA. CONS. STAT. § 6312. (ECF No. 32.)

On December 3, 2020, the court conducted a suppression hearing via Zoom video conference.[1] The government entered one exhibit into evidence, i.e., the search warrant and affidavit of probable cause, and the parties entered into a stipulation that Dish swore at the warrant before the state court judge and the state court judge and he signed it. Chretien and the government each presented argument in support of their positions.

For the reasons set forth in these findings of fact and conclusions of law, the motion to suppress will be denied.

II. FINDINGS OF FACT[2]

FOF 1. On February 5, 2019, Dish applied for a search warrant for 50 Vanadium Road, Apartment 137, Bridgeville, Pennsylvania, 15017 (the "apartment"). (Gov't Ex. A (ECF No. 29-1) at 1.)

[1] On December 3, 2020, Chretien on the record knowingly and voluntarily waived his right to an in-person suppression hearing at which he could be present before the court.

[2] For purposes of a motion to suppress, the court "may rely on hearsay and other evidence, even though that evidence would not be admissible at trial." United States v. Raddatz, 447 U.S. 667, 679 (1980); Brosius v. Warden, 278 F.3d 239, 246 n.4 (3d Cir. 2002) ("Hearsay may be considered in a suppression hearing in a federal court.") (citing Raddatz, 447 U.S. at 679)).

FOF 2. Dish listed Chretien as the occupant of the apartment. (Id.)

FOF 3. Dish listed the following items, among others, to be searched for and seized from the apartment:

> All computer hardware, including but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical similar computer impulses or data. Any computer processing units, internal and peripheral storage devise, (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives, tapes, and optical storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), and related communication devices such as modems, cables, and connections, recording equipment…any Computer processing units, internal and peripheral storage devices, (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives, tapes, and optical storage device) and any computer software…as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.
>
> …
>
> Any data, images, electronic communications, and/or any other electronic information contained on, or within, the computer system/s, computer/s, computer components, storage media, peripherals and/or computer software relating in any way [to any images, photographs or depictions of Child Pornography (as defined herein and in section 6312 of the Crimes Code).
>
> …
>
> Any data, images, electronic communications, and/or any other electronic information contained for the Screen/User account: Carol Gretski, Email accounts: gretskicarol@gmail.com, and / or mobile phone number (207)-458-5506.

(Id. at 1-2.)

FOF 4. The application pertained to a violation of 18 PA. CONS. STAT. § 6312, "Sexual Abuse of Children[.]" (Id. at 1.)

FOF 5. Dish in the affidavit of probable cause listed, among other things, his experience in law enforcement generally and with respect to the investigation of crimes involving the sexual exploitation of children. The affidavit provided that, among other things:

- Dish has twenty-five years of law enforcement experience;

- he is a member of the Delaware County Internet Crimes Against Children ("ICAC") Task Force;

- he is familiar with the investigation of the exploitation of children via the internet and in person, including the investigation of child pornography crimes;

- his experience with the investigation of child pornography crimes was obtained via training and "everyday work related to conducting" investigations of child pornography crimes; and

- he has participated in the execution of numerous search warrants for offenses of child exploitation and child pornography.

(Gov't Ex. A (ECF No. 29-1) at 3.)

FOF 6. The affidavit of probable cause provided definitions of technical terms used by Dish in the affidavit, including "Internet Protocol Address[,]" "Domain Name[,]" "Child Pornography[,]" and "American Registry of Internet Numbers (ARIN)[.]" (Id. at 3-4.)

FOF 7. The affidavit of probable cause defines "I.P. Address" as follows:

> Sometimes called a dotted quad. A unique number consisting of 4 parts separated by dots, e.g., 165.113.245.2. Every machine that is on the Internet has a unique IP number – if a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more Domain Names that are easier for people to remember.

(Gov't Ex. A (ECF No. 29-1) at 3.)

FOF 8. Dish wrote in the affidavit of probable cause that:

- Google reported to "NCMEC, Cybertips" that a person named Carol Gretski with a phone number of 207-458-5506 and email address of gretskicarol@gmail.com "uploaded an image of apparent child pornography" to be stored in "Google Photos" (id. at 4);

- Google discovered the image on two separate occasions, i.e., on May 1, 2018, and May 4, 2018 (id.);

- Google reported that on April 30, 2018, the "gretskicarol@gmail.com" user account logged onto and registered to Google from the IP address "2601:547:1280:69b4:5d72:7adf:f39f:17f9" (the "17f9 IP address") (id.);

- Dish viewed the image reported by Google, which depicted "a prepubescent female child under the age of 18 years old exposing her genitals in a sexual act and/or pose" (id.);

- on September 25, 2018, Dish applied for and received from the state court judge a search warrant for subscriber information for the 17f9 IP address on April 30, 2018, from Comcast Cable Communications LLC ("Comcast") (id.);

- Comcast responded to the search warrant that the subscriber of the 17f9 IP address was Chretien, his address of record was the apartment, the email address associated with the account was pvchretien@comcast.com, and the telephone number associated with the account was "207-458-5506" (Gov't Ex. A (ECF No. 29-1) at 4);

- on September 25, 2018, Dish applied for a received a search warrant for account information for the Google account "Carol Gretski, gretskicarol@gmail.com, phone number 2074585506" (id. at 5);

- on October 24, 2018, Google responded to the search warrant that, among other things, the 17f9 IP address was the "Terms of Service IP" associated with the account and the telephone number associated with the account was "2074585506" (id.);

- Google also provided to Dish the profile image for the gretskicarol@gmail.com account, which depicted a young, clothed female, and the image suspected to be child pornography (id.); and

- PennDOT provided that "Paul Vincent Chretien" has a valid Pennsylvania Drivers License, which lists the apartment's address. (id.)

FOF 9. Dish also wrote in the affidavit of probable cause that based upon his "knowledge, training, and experience[,]" he knows:

- records are often stored in computers and as electronic data and files on various types of media, including hard drives, zip drives, floppies, and tape drives (Gov't Ex. A (ECF No. 29-1) at 5);

- computer files and their remnants can be recovered months or years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet (id.);

- child pornographers generally prefer to store images of child pornography in electronic form as computer files (id.);

- searching and seizing information from computers often requires officers to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory (id. at 6);

- persons engaged in the distribution and possession of child pornographic materials often maintain collections of such material (id. at 6); and

- persons engaged in the distribution and possession of child pornographic materials keep their collections for long periods of times, i.e., years at a time (id.).

FOF 10. Dish concluded that based upon the foregoing, images of child pornography would be found on computers and other storage media found at the apartment in violation of section 6312. (Gov't Ex. A (ECF No. 29-1) at 6.)

FOF 11. On February 5, 2010, at 9:20 a.m., the state court judge caused a search warrant to be issued for the apartment based upon Dish's affidavit of probable cause and application for a search warrant. (Id. at 1.)

FOF 12. According to Chretien, on February 6, 2019, at approximately 7:00 a.m., the search warrant was executed at the apartment. (ECF No. 29 ¶ 2.)

FOF 13. Chretien alleges that law enforcement officers conducted an interview of him during which he made incriminating statements. (Id. ¶ 3.)

FOF 14. Chretien also alleges that on April 2, 2019, Katherine Donahue ("Donahue"), an agent for the Federal Bureau of Investigations ("FBI") obtained a search warrant authorized by a federal magistrate judge for the seizure of three email accounts maintained by Google, and, on April 11, 2019, Donahue obtained an additional search warrant for the seizure of three email accounts maintained by Google. (Id. ¶¶ 4-5.)

FOF 15. Chretien attached to his suppression motion a "Receipt for Property…Seized" form from the United States Department of Justice, Federal Bureau of Investigation, with his name and address on it dated February 6, 2019. (ECF No. 29-1 at 7.)

FOF 16. In the section of the form entitled "Description of Item(s):" there are several items listed, but the entirety of the section is not legible. (Id.)

III. CONCLUSIONS OF LAW

COL 1. The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…." U.S. CONST. AMEND. IV.

COL 2. Chretien argues that the evidence obtained pursuant to the search warrant issued by the state court judge for his apartment should be suppressed because the evidence was obtained in violation of his Fourth Amendment rights.

COL 3. Because Chretien's apartment was searched pursuant to a search warrant issued by a state court judge,[3] the court must only determine whether the judge had a "'substantial basis for… conclud[ing]' that probable cause existed.'" United States v. Conley, 4 F.3d 1200, 1205 (3d Cir. 1993) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

COL 4. The Third Circuit Court of Appeals has explained:

> This standard "does not mean that reviewing courts should simply rubber stamp a magistrate's conclusions." United States v. Tehfe, 722 F.2d 1114, 1117 (3d Cir.1983), cert. denied sub nom., Sanchez v. United States, 466 U.S. 904, 104 S.Ct. 1679, 80 L.Ed.2d 154 (1984). Nevertheless, the role of the reviewing court is quite limited. The Supreme Court has directed that "although in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." United States v. Ventresca, 380 U.S. 102, 109, 85 S.Ct. 741, 746, 13 L.Ed.2d 684 (1965) (emphasis

[3] The "substantial basis standard" discussed below applies to determinations of probable cause made by federal magistrate judges and state court judges. See United States v. Miknevich, 638 F.3d 178, 182 n.4 (3d Cir. 2011) (explaining that the "substantial basis" standard applied "to any member of the judiciary—federal or state—who has the authority to issue warrants").

> added), quoted with approval in Gates, 462 U.S. at 237 n. 10, 103 S.Ct. at 2331 n. 10.

Conley, 4 F.3d at 1205.

COL 5. "Probable cause exists when 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" United States v. Grubbs, 547 U.S. 90, 96 (2006) (quoting Gates, 462 U.S. at 238). Probable cause determinations require the issuing judge to make a "practical, common-sense decision." Gates, 462 U.S. at 238. "The supporting affidavit must be read in its entirety and in a common sense and nontechnical manner." Conley, 4 F.3d at 1206 (citing Gates, 462 U.S. at 230–31).

COL 6. In the context of a child pornography case, the Third Circuit Court of Appeals has recognized that "evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address." United States v. Vosburgh, 602 F.3d 512, 526 (3d Cir. 2010) (citing United States v. Perez, 484 F.3d 735 (5th Cir.2007)).

COL 7. The court of appeals in Vosburgh explained that IP addresses are unique identifiers that are traceable to physical addresses. Id. In that case, law enforcement learned that a particular IP address attempted to access child pornography three times. Id. at 518. The court of appeals recognized that attempted possession of child pornography is a federal crime. Id. at 527. Law enforcement traced the IP address to a physical location, i.e., the defendant's apartment. Id. at 518. The affidavit of probable cause detailed, among other things, that persons engaged in child pornography offenses typically store their large collections of child pornography in their homes and on computer devices, and even if images of child pornography are deleted from a computer's hard drive, law enforcement can retrieve the images with the use of forensic tools. Vosburgh, 602 F.3d at 518. The court held that under those circumstances, there was a fair probability that

instrumentalities of the crime, i.e., attempted possession of child pornography, would be found in the defendant's apartment. Id. at 527.

COL 8. Here, Dish had information that child pornography was possessed at the apartment in violation of section 6312.

COL 9. One court has explained:

> To find probable cause for an 18 Pa.C.S. § 6312 violation, law enforcement must supply facts or circumstances in an affidavit that would lead one to reasonably believe that a suspect photographed, disseminated photographs, intentionally viewed or knowingly possessed photos of a "child under the age of 18 years engaging in a prohibited sexual act." 18 Pa.C.S. § 6312(b)(d)….In pertinent part, § 6312(g) defines a "prohibited sexual act," as including "nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view such depiction." 18 Pa.C.S. § 6312(g) (emphasis added).

United States v. Kofalt, No. CRIM. 11-155, 2012 WL 5398832, at *7 (W.D. Pa. Nov. 2, 2012), aff'd, 668 F. App'x 426 (3d Cir. 2016) (footnote omitted).[4]

COL 10. The affidavit of probable cause provided that on May 1, 2018, and May 4, 2018, Google discovered that the account of gretskicarol@gmail.com, which was registered with Google on April 30, 2018, uploaded an image of child pornography to "Google Photos." Google reported its discoveries to law enforcement. Dish learned that the gretskicarol@gmail.com account utilized the 17f9 IP address. Dish in the affidavit explained that an IP address is a "unique" set of numbers associated with a machine connected to the internet. Dish learned that "Paul Chretien"

---

[4] The court in Kofalt recognized that section 6312 prohibits more conduct than its federal counterpart, 18 U.S.C. § 2252, under which Chretien was indicted in this case. The court explained:

> Comparing the language of the two statutes, the state statute plainly criminalizes a broader scope of conduct than the federal statute upon which Defendant relies. A violation of the Pennsylvania statute requires only a naked picture of a minor, while the image must be more explicit to violate the Federal statute.

Kofalt, 2012 WL 5398832, at *7.

subscribed to the 17f9 IP address via Comcast. The physical address associated with the Comcast account was the apartment, the email address of record was pvchretien@comcast.com, and the telephone number associated with the account was the same telephone number provided to Google with respect to thegretskicarol@gmail.com account. Dish discovered that Chretien's driver license listed the apartment's address.

COL 11. Based upon the foregoing, Dish's affidavit of probable cause showed that the gretskicarol@gmail.com account uploaded images of child pornography to "Google Photos" via the 17f9 IP address and the 17f9 IP address was issued to Chretien who listed the apartment as his address with Comcast and PennDOT.

COL 12. Chretien argues, however, that the information contained in the affidavit of probable cause with respect to his possession of child pornography was stale because nine months passed from when Google reported the images of child pornography were uploaded to "Google Photos" in May 2018, to the issuance of the search warrant on February 5, 2019.

COL 13. The government argues in response that the information was not stale because—as Dish provided in the affidavit of probable cause—persons engaged in violations of section 6312 maintain collections of child pornography, and, even if images are deleted, they can be retrieved by technology experts.

COL 14. "The concept of staleness is important in determining probable cause for a search." United States v. Tehfe, 722 F.2d 1114, 1119 (3d Cir.1983). In "[a]n application for a search warrant…it is necessary to establish that certain items are probably located at the present time in a certain place." Id. "It is not enough that the items may have been at the specified location at some time in the past—there must be probable cause to believe that they are there when the warrant issues." Id. "The likelihood that the evidence sought is still in place depends on a number

of variables, such as the nature [1] of the crime, [2] of the criminal, [3] of the thing to be seized, and [4] of the place to be searched." Id.

COL 15. In the context of child pornography crimes, it is well-recognized (including by Dish in the affidavit) that "persons with an interest in child pornography tend to hoard their materials and retain them for a long time." Vosburgh, 602 F.3d at 528. "Child pornography is illegal, and therefore difficult and risky to obtain. Presumably, once a child pornography collector gets his hands on such material he will not be quick to discard it." Id. Although evidence of child pornography crimes may—at some point—grow stale, courts consider the evidence to have a "long shelf life" and "[i]t has not been, and should not be, quickly deemed stale." Id. at 529 (collecting decisions). "This is especially true where, as here, the crime in question is accomplished through the use of a computer." Id.

COL 16. As Dish also recognized in his affidavit, "[i]mages stored on computers can be retained almost indefinitely, and forensic examiners can often uncover evidence of possession or attempted possession long after the crime has been completed." Id.

COL 17. In light of the foregoing principles about the nature of child pornography crimes and the things to be seized with respect to those crimes, the court of appeals in Vosburgh held that a lapse of time of *four months* from when the defendant in that case attempted to possess child pornography and when the search warrant was executed did not render the information in the affidavit of probable cause stale. Vosburgh, 602 F.3d at 529.

COL 18. The court of appeals in Vosburgh supported its holding with United States v. Shields, 458 F.3d 269, 279 (3d Cir. 2006), in which it held that a lapse of ***nine months*** between law enforcement's discovery of the possession of child pornography and the execution of a search

warrant did not render evidence of the possession of child pornography stale. Id. at 528-29. The court of appeals Vosburgh explained:

> In Shields, FBI agents infiltrated two online groups explicitly dedicated to the exchange of child pornography. Eventually, both groups were shut down and the agents obtained records of group members' email addresses. Shields, 458 F.3d at 272. They traced one of those addresses back to Shields. Nine months after the groups were shut down, agents obtained a search warrant for Shields's home, where they found hundreds of images of child pornography. Id. at 273. On appeal, we rejected Shields's probable cause challenge. Shields did not argue staleness, but we raised the issue sua sponte and concluded that the information in the affidavit was not stale, despite the nine-month gap between the warrant application and any possible participation by Shields in the child pornography groups. Id. at 279 n. 7.

Vosburgh, 602 F.3d at 528.

COL 19. Here, as explained above, the affidavit of probable cause connected the possession of images of child pornography by the gretskicarol@gmail.com account to the apartment.

COL 20. The affidavit of probable cause also provided that Dish knew based upon his training and experience with respect to child pornography crimes that: (1) child pornographers generally prefer to store images of child pornography in electronic form as computer files; (2) persons engaged in the distribution and possession of child pornographic materials often maintain collections of such material; (3) persons engaged in the distribution and possession of child pornographic materials keep their collections for long periods of times, i.e., years at a time; and (4) computer files and their remnants can be recovered months or years after they have been downloaded onto a hard drive, deleted, or viewed via the internet.

COL 21. Based upon the foregoing information that was included in the affidavit of probable cause, Dish's information that child pornography was possessed at the apartment was not stale because the nature of child pornography crimes (as described above) and the specifics of this

case, i.e., child pornography was stored on the internet via the gretskicarol@gmail.com "Google Photos" account.

COL 22. The state court judge, therefore, had a substantial basis to conclude that on February 5, 2019, there was a fair probability that evidence of a violation of section 6312, i.e., possession of child pornography, would be found at the apartment. The court, therefore, need not address whether the good faith exception or the fruit of the poisonous tree doctrine apply in this case.

III. CONCLUSION

For the reasons set forth in this opinion, the motion to suppress evidence (ECF No. 29) filed by Chretien will be denied.

An appropriate order will be entered.

BY THE COURT,

DATED: December 21, 2020

/s/ JOY FLOWERS CONTI
Joy Flowers Conti
Senior United States District Judge